(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 2000010927 A

(43) Date of publication of application: 14 . 01 . 00

(51) Int. Cl G06F 15/00
H04Q 7/38
H04L 9/32
H04L 12/28
H04M 1/66
H04M 11/00

(21) Application number: 10178410

(22) Date of filing: 25 . 06 . 98

(71) Applicant: NEC YONEZAWA LTD

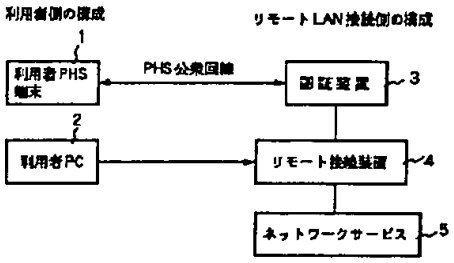
(72) Inventor: KATOU MASARU

(54) AUTHENTICATION SYSTEM AND DEVICE

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a fast and highly reliable authentication system and also to provide an inexpensive authentication device.

SOLUTION: An authentication device 3 manages a user password request/ notification function for a user, issues a temporary password against a connection request of the user and notifies a user PHS terminal 1 and a remote connection device 4 of the temporary password. The device 4 accepts a connection request from a user PC 2 based on the temporary password and performs the remote connection of a normal user or an inquiring user to an authentication device 3. The PC 2 performs connection to the device 4 based on the temporary password. The network service 5 is the network resources with which every user enjoys the service.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－10927
（P2000－10927A）
(43)公開日　平成12年１月14日(2000.1.14)

(51)Int.Cl.'		識別記号	FI			テーマコード'(参考)
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ	15/00	３３０Ｂ	５Ｂ０８５
Ｈ０４Ｑ	7/38		Ｈ０４Ｍ	1/66	Ｂ	５Ｊ１０４
Ｈ０４Ｌ	9/32			11/00	３０３	５Ｋ０２７
	12/28		Ｈ０４Ｂ	7/26	１０９Ｓ	５Ｋ０３３
Ｈ０４Ｍ	1/66		Ｈ０４Ｌ	9/00	６７３Ａ	５Ｋ０６７

審査請求 有　請求項の数６　ＯＬ　（全７頁）　最終頁に続く

(21)出願番号　特願平10－178410

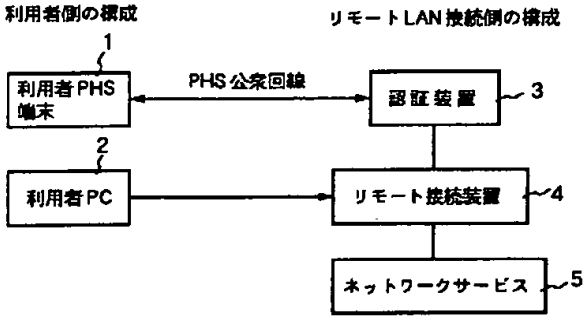
(22)出願日　平成10年６月25日(1998.6.25)

(71)出願人　000240617
米沢日本電気株式会社
山形県米沢市下花沢２丁目６番80号
(72)発明者　花等　勝
山形県米沢市下花沢２丁目６番80号　米沢日本電気株式会社内
(74)代理人　100085235
弁理士　松浦　兼行

最終頁に続く

(54)【発明の名称】　認証システム及び認証装置

(57)【要約】
【課題】　従来の認証システムでは、変化するパスワードを作成／管理する装置（ワンタイムパスワード生成カード及び認証装置）が非常に高価であるため、大規模な普及には至っていない。
【解決手段】　認証装置３は、利用者における「利用者パスワード要求／通知機能」の管理と、利用者からの接続要求に対し「一時的なパスワード」の発行と、「一時的なパスワード」を利用者ＰＨＳ端末１とリモート接続装置４への通知とを実行する。リモート接続装置４は、「一時的なパスワード」を基に利用者ＰＣ２からの接続要求を受け付け、認証装置３に対して正規ユーザか問い合わせ利用者のリモート接続を行う。利用者ＰＣ２は、「一時的なパスワード」に基づいて、リモート接続装置４に対して接続を行う。ネットワークサービス５は各利用者がサービスを受けるネットワークの資源である。



1

【特許請求の範囲】

【請求項１】　利用者の正当性を確認してから当該利用者のパーソナルコンピュータからネットワークサービスの資源の利用を許可する認証システムにおいて、

前記利用者の簡易型携帯電話端末と、

前記簡易型携帯電話端末の電話番号とパスワードとリモート接続ＩＤを予め登録し、前記パスワードとリモート接続ＩＤを前記利用者に通知し、前記利用者の簡易型携帯電話端末からの電話番号とパスワードを受け、予め登録してある前記電話番号とパスワードと比較して一致するときは、一時的なパスワードを前記利用者の簡易型携帯電話端末に発行する認証装置と、

前記簡易型携帯電話端末への前記一時的なパスワードの通知により前記利用者が前記パーソナルコンピュータを用いて行う接続要求を受け、前記認証装置に対し前記パスワードと前記リモート接続ＩＤが正しいか問い合わせ、前記認証装置より正しいと通知された時のみ前記パーソナルコンピュータと前記ネットワークサービスを接続させるリモート接続装置とを有することを特徴とする認証システム。

【請求項２】　前記利用者は、前記パーソナルコンピュータを使用して、前記認証装置から通知された前記リモート接続ＩＤと前記一時的なパスワードとを使用して前記リモート接続装置に接続要求を行うことを特徴とする請求項１記載の認証システム。

【請求項３】　前記認証装置は前記リモート接続装置からの問い合わせに対して、前記利用者に発行した情報と前記リモート接続装置からの情報とが一致するか判断し、その判断結果を前記リモート接続装置に通知することを特徴とする請求項１記載の認証システム。

【請求項４】　前記携帯電話端末は、前記認証装置からの前記一時的なパスワード通知前に電源をオフすることを特徴とする請求項１記載の認証システム。

【請求項５】　利用者の正当性を確認してから当該利用者のパーソナルコンピュータからネットワークサービスの資源の利用を許可する認証システムに用いる認証装置において、

前記利用者の簡易型携帯電話端末の電話番号とパスワードとリモート接続ＩＤを予め登録し、前記パスワードとリモート接続ＩＤを前記利用者に通知し、前記利用者の簡易型携帯電話端末からの電話番号とパスワードを受け、予め登録してある前記電話番号とパスワードと比較して一致するときは、一時的なパスワードを前記利用者の簡易型携帯電話端末に発行し、リモート接続装置からの問い合わせに対して正しいと判断した時は、前記リモート接続装置により前記パーソナルコンピュータと前記ネットワークサービスを接続させることを特徴とする認証装置。

【請求項６】　前記リモート接続装置からの問い合わせに対して、前記利用者に発行した情報と前記リモート接続装置からの情報とが一致するか判断し、その判断結果を前記リモート接続装置に通知することを特徴とする請求項５記載の認証装置。

2

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は認証システム及び認証装置に係り、特にローカルエリアネットワーク（ＬＡＮ）サービスの提供を正規の利用者に対してのみ許可する認証システム及び認証装置に関する。

【０００２】

【従来の技術】ＬＡＮにおける相互の計算機のサービスを利用するネットワークサービス機能として、一般に送信されてくるログイン計算機の利用者識別子（ＩＤ、パスワード）を用いて、リモート資源の利用権を検査する認証機能がある。ネットワーク接続計算機システムでは、利用者識別子は計算機利用開始時にネットワーク計算機システムを構成する各計算機上の利用者登録リストを用いて、各計算機上のシステムソフトウェアにより与えられている。また、パーソナルハンディホンシステム（ＰＨＳ）端末を利用した国際電話利用システムにおいて、ＩＤ番号とパスワードを用いてシステムを呼び出し、正当性確認後はシステム側からのコールバック機能を利用するシステムも知られている（特開平９－１３５２９５号公報）。

【０００３】しかし、この方法では利用者のＩＤやパスワードが第三者に盗まれると、許可されていない第三者がネットワークサービスに侵入できる危険性を持っている。そこで、近年は一定時間毎に変化するパスワードを利用した認証システムが提案され、既に実用化されている。この従来の認証システムでは、パスワードが一定時間毎に変化するので、第三者によるパスワードの盗用を困難にできる。

【０００４】

【発明が解決しようとする課題】しかるに、上記の従来の認証システムでは、変化するパスワードを作成／管理する装置（ワンタイムパスワード生成カード及び認証装置）が非常に高価であるため、大規模な普及には至っていないという問題がある。

【０００５】本発明は以上の点に鑑みなされたもので、高速で高信頼性な認証システム及び安価な認証装置を提供することを目的とする。

【０００６】また、本発明の他の目的は、生産性や保守性、資源の再利用性が可能な認証システム及び認証装置を提供することにある。

【０００７】更に、本発明の他の目的は、小型で軽量な認証装置を提供することにある。

【０００８】

【課題を解決するための手段】上記の目的を達成するため、本発明の認証システムは、利用者の正当性を確認してから当該利用者のパーソナルコンピュータからネット

ワークサービスの資源の利用を許可する認証システムにおいて、利用者の簡易型携帯電話端末と、簡易型携帯電話端末の電話番号とパスワードとリモート接続ＩＤを予め登録し、パスワードとリモート接続ＩＤを利用者に通知し、利用者の簡易型携帯電話端末からの電話番号とパスワードを受け、予め登録してある電話番号とパスワードと比較して一致するときは、一時的なパスワードを利用者の簡易型携帯電話端末に発行する認証装置と、簡易型携帯電話端末への一時的なパスワードの通知により利用者がパーソナルコンピュータを用いて行う接続要求を受け、認証装置に対しパスワードとリモート接続ＩＤが正しいか問い合わせ、認証装置より正しいと通知された時のみ前記パーソナルコンピュータとネットワークサービスを接続させるリモート接続装置とを有することを特徴とする。

【０００９】また、本発明の認証システムは、上記の目的を達成するため、利用者の正当性を確認してから当該利用者のパーソナルコンピュータからネットワークサービスの資源の利用を許可する認証システムに用いる認証装置において、利用者の簡易型携帯電話端末の電話番号とパスワードとリモート接続ＩＤを予め登録し、パスワードとリモート接続ＩＤを利用者に通知し、利用者の簡易型携帯電話端末からの電話番号とパスワードを受け、予め登録してある電話番号とパスワードと比較して一致するときは、一時的なパスワードを利用者の簡易型携帯電話端末に発行し、リモート接続装置からの問い合わせに対して正しいと判断した時は、リモート接続装置によりパーソナルコンピュータとネットワークサービスを接続させる構成としたものである。

【００１０】本発明では、認証装置に登録した携帯電話端末だけが持つセキュリティと、利用者が携帯型電話端末に他するパスワードを管理することのセキュリティと、認証装置が一時的なパスワードを決められた利用者の携帯電話端末に送ることのセキュリティを組み合わせたセキュリティをもつことができる。

【００１１】また、本発明ではＰＨＳ端末のような一般市販の簡易型携帯電話端末を使用して認証許可を得ることができる。

【００１２】

【発明の実施の形態】次に、本発明の実施の形態について図面と共に説明する。図１は本発明になる認証システムの一実施の形態のブロック図を示す。同図において、利用者のパーソナルハンディホンシステム（ＰＨＳ）端末１と、利用者のパーソナルコンピュータ（ＰＣ）２と、ＰＨＳ端末１とＰＨＳ公衆回線を介して接続される認証装置３と、利用者ＰＣ２と認証装置３に接続されたリモート接続装置４と、リモート接続装置４が提供するネットワークサービス５とからなる。リモートＬＡＮ接続側の構成は、認証装置３、リモート接続装置４及びネットワーク５からなる。

【００１３】認証装置３は利用者の正当性を確認する装置であり、利用者における「利用者パスワード要求／通知機能」の管理と、利用者からの接続要求に対し「一時的なパスワード」の発行と、「一時的なパスワード」を利用者パスワード要求／通知機能を持つ利用者ＰＨＳ端末１と、リモート接続機能を持つリモート接続装置４への通知とを実行する。

【００１４】リモート接続装置４は、認証装置３から発行された「一時的なパスワード」を基に、利用者接続用計算機システムである利用者ＰＣ２からの接続要求を受け付け、認証装置３に対して正規ユーザか問い合わせ利用者のリモート接続を行う。利用者ＰＨＳ端末１は、利用者パスワード要求／通知機能を有する一般市販の簡易型携帯電話機であり、利用者が認証装置３に対して「一時的なパスワード」を要求し、正しく認証されれば、認証装置から「一時的なパスワード」が通知される。「一時的なパスワード」は予め定められた特定のものではなく、要求の都度適宜設定されるパスワードである。

【００１５】利用者接続用計算機システムである利用者ＰＣ２は、認証装置から利用者ＰＨＳ端末１に通知された「一時的なパスワード」に基づいて、リモート接続装置４に対して接続を行う。ネットワークサービス５は各利用者がサービスを受けるネットワークの資源である。

【００１６】次に、この実施の形態の動作について図２のフローチャートを併せ参照して説明する。まず、認証装置３に利用者のＰＨＳ端末１のＰＨＳ番号、認証装置パスワード及びリモート接続ＩＤを登録する（ステップ１１）。続いて、認証装置パスワード及びリモート接続ＩＤをあらかじめ利用者に通知する（ステップ１２）。続いて、利用者は利用者ＰＨＳ端末１から認証装置３に対して電話（ＴＥＬ）をかける（ステップ１３）。電話をかける方法は、例えば「認証装置電話番号＃認証装置パスワード」の数字列である。例えば０２３８２１１２３４＃ＡＢＣＤである。

【００１７】次に、認証装置３は利用者ＰＨＳ端末１からの電話を受け、利用者ＰＨＳ番号と認証装置パスワードを確認し（ステップ１４）、それらの値がステップ１１での登録情報と一致しているかどうか判断し、一致していれば利用者ＰＨＳ端末１に対し、「これからパスワードを発行します。電源を切ってお待ち下さい。」等の音声メッセージで答える（ステップ１５）。なお、音声メッセージ以外の文字メッセージその他の方法も可能である。

【００１８】次に、利用者は上記の音声メッセージに従い、利用者ＰＨＳ端末１の電源をオフにする（ステップ１６）。続いて、認証装置３は、利用者ＰＨＳ端末１に対し、「一時的なパスワード」を発行し、利用者ＰＨＳ端末１に文字メッセージで通知する（ステップ１７）。この場合、きゃらめーる等のサービスを利用する。一時的なパスワードは、例えばＶＷＸＹＺとする。

5

【００１９】上記の一時的なパスワード「ＶＷＸＹＺ」が利用者のＰＨＳ端末１に通知されると（ステップ１８）、利用者はリモート接続装置４に対してネットワーク接続要求を行う（ステップ１９）。すなわち、利用者ＰＣ２を使用してリモート接続装置４に対してダイヤルアップを行う。この場合、ＩＤはステップ１１で入手したＩＤ、パスワードはステップ１８で入手した「一時的なパスワード」を使用する。例えば、ＩＤは「ＳＵＺＵＫＩ」であり、一時的なパスワードは「ＶＷＸＹＺ」である。

【００２０】続いて、リモート接続装置４は利用者ＰＣ２から接続要求を受けると（ステップ２０）、認証装置３に対してユーザＩＤ及びパスワードが正しいかどうか問い合わせる（ステップ２１）。すると、認証装置３はリモート接続装置４からの問い合わせに対して利用者に発行した情報と一致するか判断する（ステップ２２）。上記のステップ２２で認証装置３が一致しているとの判断をした場合、その判断結果をリモート接続装置４に通知し、これによりリモート接続装置４はネットワークサービス５の利用を利用者に対して許可し、利用者ＰＣ２とネットワークサービス５との接続を行う（ステップ２３）。

【００２１】これにより、利用者ＰＣ２からネットワークサービス５の資源が利用可能となる（ステップ２４）。なお、認証装置３がステップ２２で不一致の判断結果を得た場合、リモート接続装置４はその判断結果を受け、利用者に対するネットワークサービス５の提供を拒否する。

【００２２】このように、この実施の形態では、ＰＨＳ端末１が自分のＰＨＳ番号を通知する機能があることを利用して、利用者が認証装置３に登録したＰＨＳ端末１だけを認証することで、他のＰＨＳ端末ではなりすましができにくいというセキュリティと、利用者のＰＨＳ端末１が例え盗難に遭っても、パスワードを知らないと認証装置３に接続できないため、利用者がＰＨＳ端末１に対するパスワードを管理することのセキュリティと、正しいＰＨＳ端末１に認証装置３が一時的なパスワードを発行することのセキュリティの組み合わせにより、非常に強固なセキュリティを持つため、第三者が不正にネットワークサービス５を利用することは極めて困難にできる。

【００２３】また、利用者ＰＨＳ端末１は市販のＰＨＳ

6

端末であり、小型、軽量、低消費電力の端末を利用できると共に、操作性が簡単であり、またこの実施の形態では、ＰＨＳ公衆回線のインフラストラクチャを使用するので、高速・伝送効率の向上・高信頼性のデータ転送ができ、更にシステム全体の費用の削減も出切る。また、ＰＨＳの高速通信機能（ＰＩＡＦＳ）を利用したサービスも可能となる。更に、この実施の形態では市販のＰＨＳ端末を利用することにより、量産効果のため価格が低く設定されており、生産性、保守性も高く、未使用ＰＨＳ端末を使用することによる資源の再利用も可能である。

【００２４】

【発明の効果】以上説明したように、本発明によれば、認証装置に登録した携帯電話端末だけが持つセキュリティと、利用者が携帯型電話端末に他するパスワードを管理することのセキュリティと、認証装置が一時的なパスワードを決められた利用者の携帯電話端末に送ることのセキュリティを組み合わせたセキュリティをもつようにしたため、従来に比べて非常に強固なセキュリティを向上できる。

【００２５】また、本発明によれば、ＰＨＳ端末のような一般市販の簡易型携帯電話端末を使用して認証許可を得るようにしているため、ＰＨＳ公衆回線のインフラストラクチャを使用でき、よって高速・伝送効率向上・高信頼性のデータ転送ができる。更に、本発明によれば、ＰＨＳ端末のような一般市販の簡易型携帯電話端末を使用しているので、端末として小型・軽量・低消費電力の端末や、生産性、保守性が高く、操作性も簡単な端末を使用でき、未使用ＰＨＳ端末を使用することによる資源の再利用もでき、ひいてはシステム全体の費用を削減でき、高速通信機能を利用したサービスも受けることができる。

【図面の簡単な説明】

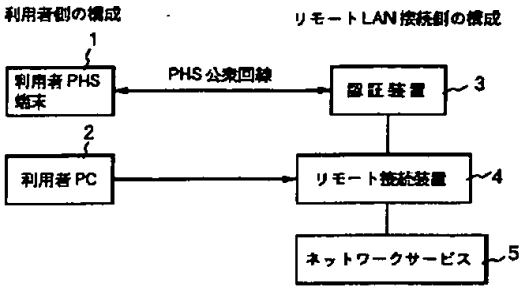
【図１】本発明の一実施の形態のブロック図である。

【図２】本発明の一実施の形態のフローチャートである。

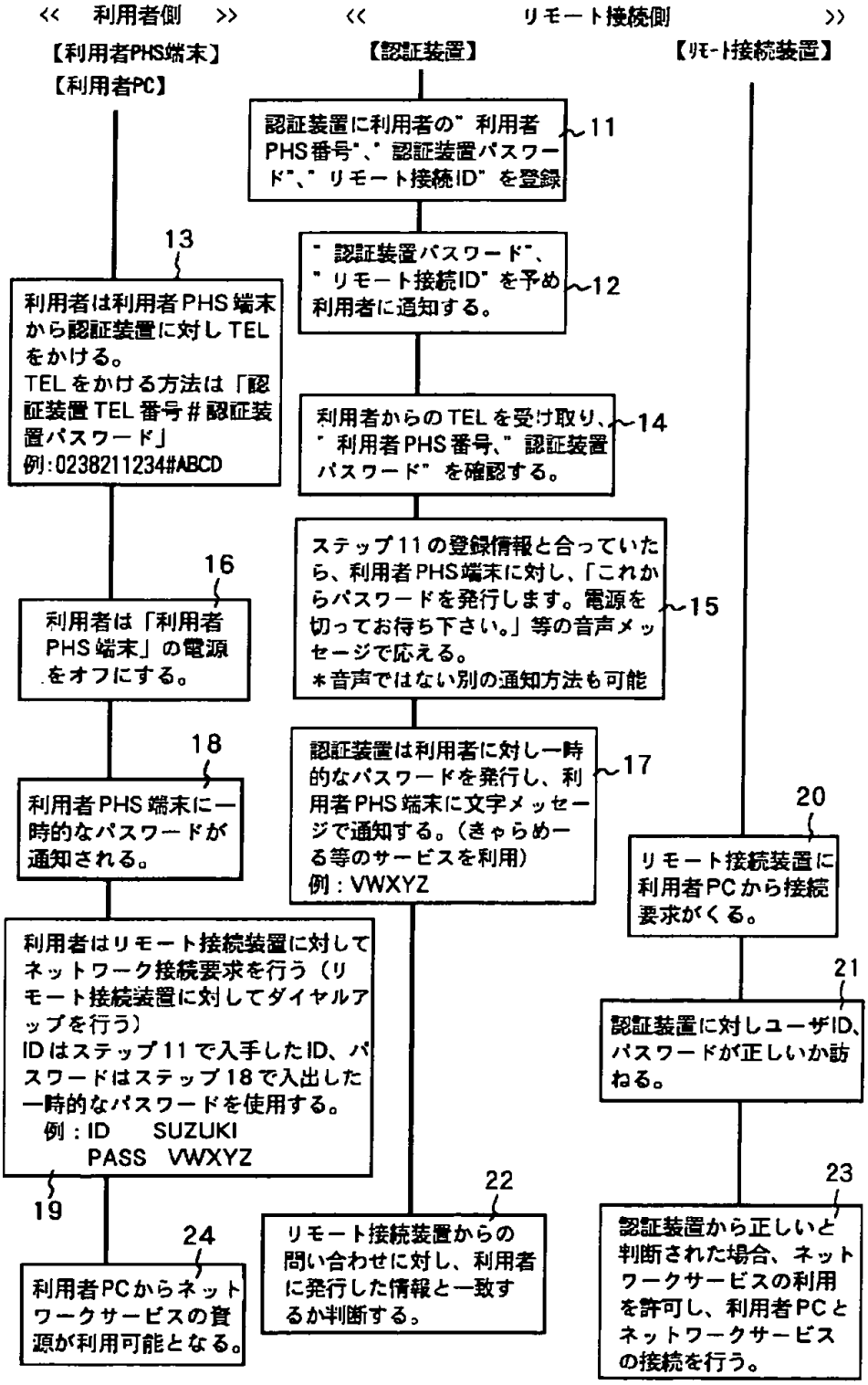
【符号の説明】

１　利用者のＰＨＳ端末
２　利用者のパーソナルコンピュータ（ＰＣ）
３　認証装置
４　リモート接続装置
５　ネットワークサービス

【図１】


利用者側の構成
リモートLAN接続側の構成
1
利用者PHS端末
PHS公衆回線
認証装置
3
2
利用者PC
リモート接続装置
4
ネットワークサービス
5

【図2】


<< 利用者側 >>
【利用者PHS端末】
【利用者PC】
<< 【認証装置】
リモート接続側 >>
【リモート接続装置】
認証装置に利用者の" 利用者PHS番号"、" 認証装置パスワード"、" リモート接続ID" を登録
11
" 認証装置パスワード"、" リモート接続ID" を予め利用者に通知する。
12
13
利用者は利用者PHS端末から認証装置に対しTELをかける。
TELをかける方法は「認証装置TEL番号#認証装置パスワード」
例:0238211234#ABCD
利用者からのTELを受け取り、" 利用者PHS番号、" 認証装置パスワード" を確認する。
14
ステップ11の登録情報と合っていたら、利用者PHS端末に対し、「これからパスワードを発行します。電源を切ってお待ち下さい。」等の音声メッセージで応える。
＊音声ではない別の通知方法も可能
15
16
利用者は「利用者PHS端末」の電源をオフにする。
認証装置は利用者に対し一時的なパスワードを発行し、利用者PHS端末に文字メッセージで通知する。(きゃらめーる等のサービスを利用)
例：VWXYZ
17
18
利用者PHS端末に一時的なパスワードが通知される。
20
リモート接続装置に利用者PCから接続要求がくる。
利用者はリモート接続装置に対してネットワーク接続要求を行う(リモート接続装置に対してダイヤルアップを行う)
IDはステップ11で入手したID、パスワードはステップ18で入出した一時的なパスワードを使用する。
例：ID SUZUKI
PASS VWXYZ
19
21
認証装置に対しユーザID、パスワードが正しいか訪ねる。
22
23
リモート接続装置からの問い合わせに対し、利用者に発行した情報と一致するか判断する。
認証装置から正しいと判断された場合、ネットワークサービスの利用を許可し、利用者PCとネットワークサービスの接続を行う。
24
利用者PCからネットワークサービスの資源が利用可能となる。

フロントページの続き

(51) Int. Cl.⁷	識別記号	F I	ﾃｰﾏｺｰﾄﾞ (参考)
H04M 11/00	303	H04L 11/00	310Z 5K101

Fターム(参考)　5B085 AA01 AC01 AE01 AE15 AE21
AE23 BG07 CE08
5J104 AA03 AA07 EA01 EA03 EA20
KA01 NA21 PA07
5K027 AA11 BB09 BB14 CC08
5K033 AA08 BA04 CB01 DB12 DB14
DB20 EC03
5K067 AA35 BB32 FF00 KK13
5K101 LL12

THIS PAGE BLANK (USPTO)

THIS PAGE BLANK (USPTO)